Smart Grid Architecture Committee Standard Review Form

Standard Name	Guidelines for. Smart Grid Cyber Security
Standard Number	NISTIR 7628 volumes 1, 2, & 3
Standard Development Organization	National Institute of Standards and Technology (NIST)
Document Type (as defined by Standard organization)	Interagency Report
Priority Action Plan	NA
URI to Specification	http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

1. *Scope as stated in the Standard:*

The three-volume report, NISTIR 7628, Guidelines for Smart Grid Cyber Security1, presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of Smart Grid stakeholders—from utilities to providers of energy management services to manufacturers of electric vehicles and charging stations—can use the methods and supporting information presented in the report as guidance for assessing risk, and then identifying and applying appropriate security requirements to mitigate that risk. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cyber security requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

2. *Purpose as stated in the Standard:*

Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…"

Effective cyber security is integral to achieving a nationwide Smart Grid, as explicitly recognized in EISA.2

> *It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure*

> *electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:*
>
> *(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.*
>
> *(2) Dynamic optimization of grid operations and resources, with full cyber-security.*

3. Are the scope and purpose aligned with the actual standard?

The Report provides a comprehensive catalogue of the different types of cyber threats that practitioners should be aware of as the current grid is evolved into a smart grid. It does not provide a map of how to address each issue, as it shouldn't, but does provide a nomenclature to describe the threats and a check-list for completeness.

Volume 2 catalogues concerns related to personal privacy in residences touched by the smart grid.

The report does not address whether some issues should present themselves under the model Architecture for the smart grid. Better architectural segmentation of the smart grid will change praxis, and thus invalidate some portions of this report for future work.

Many issues facing current installations would present themselves differently if the architecture outlined in the various reference architectures were in place. Not all interactions need to be hard-wired. There are limited number of interactions, such as domain-required timing, wherein future choices will remain constrained. Other interfaces can and will be implemented in several ways.

This report provides design guidance, rather than mandating specific design. Users of this report will be aware of issues that arise with current design and deployments, and it should be read with this in mind.

The SGAC should use this report to draw its own attention to areas wherein the deployed architecture itself creates the security issues catalogued, and use that to improve and accelerate its own work. This can then provide guidance back to assist the Cybersecurity team to provide more directed advice in future versions.

The actual report does address the scope and purpose it title suggests.

4. SGAC team summary of purpose and scope

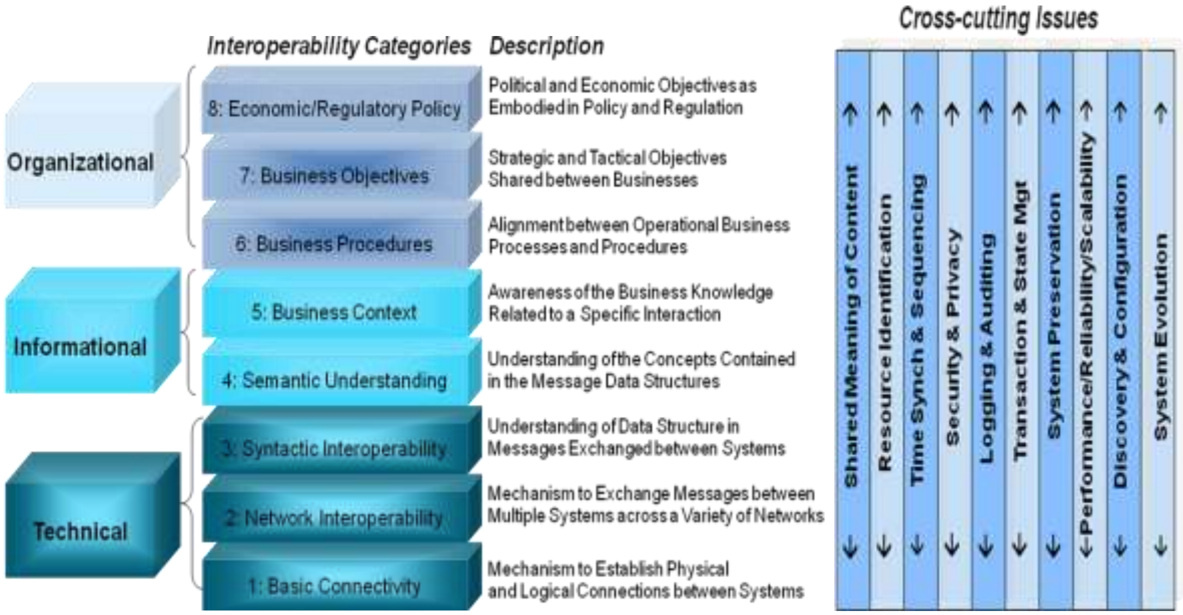
The report provides a comprehensive catalogue of the interactions of systems being deployed today. For each item in the catalogue, the interactions that a cyber-security plan should address are named. The report catalogues the systems of the day, without looking to the architecture planned for tomorrow's systems.

5. What Conceptual Model Domains are affected:

Markets	Y
Operations	Y
Service Providers	Y
Bulk Generation	Y
Transmission	Y
Distribution	Y
Customer	Y

6. What Levels in the ISO 7 Layer Model and/or the GWAC Stack are affected by the standard?

Application	
Presentation	X
Session	X
Transport	X
Network	X
Data Link	X
Physical	X


Cross-cutting Issues
Interoperability Categories
Description
Organizational
Informational
Technical
8: Economic/Regulatory Policy
Political and Economic Objectives as Embodied in Policy and Regulation
7: Business Objectives
Strategic and Tactical Objectives Shared between Businesses
6: Business Procedures
Alignment between Operational Business Processes and Procedures
5: Business Context
Awareness of the Business Knowledge Related to a Specific Interaction
4: Semantic Understanding
Understanding of the Concepts Contained in the Message Data Structures
3: Syntactic Interoperability
Understanding of Data Structure in Messages Exchanged between Systems
2: Network Interoperability
Mechanism to Exchange Messages between Multiple Systems across a Variety of Networks
1: Basic Connectivity
Mechanism to Establish Physical and Logical Connections between Systems
Shared Meaning of Content
Resource Identification
Time Synch & Sequencing
Security & Privacy
Logging & Auditing
Transaction & State Mgt
System Preservation
Performance/Reliability/Scalability
Discovery & Configuration
System Evolution

The report addresses potentially every level of the GWAC stack, because it addresses security (levels 1-7) and privacy (5-8).

7. **If the standard addresses multiple layers… Why? Is there effective separation of layers (in the ISO or GWAC stack)? Is there a plan to migrate to single layer standard?**

Security is cross-cutting, and failure of security at any level, whether interference with signal, interception of message, or misuse of information is of concern to cyber security. There is no plan to migrate to a single level standard.

8. **How would technology based on the standard be used in applications in the future? Adapted to today's applications?**

The report is well adapted to improving the cyber security of current systems and the ones soon to be deployed. The report was developed independent to the reference architecture (s) for the smart grid and therefore has some areas that should be made in better alignment to support future systems and business models.

9. **Is there a migration path from current use in the area of the standard to this standard?**

The primary use of this report is to support movement from today's current usage to more secure deployments.

10. **Does this standard affect any other PAP (if yes, list)?**

~~While the~~The advice and ~~catalogues herein should be used~~catalogue of issues in NISTIR 7628 apply to all information exchanges, communications~~,~~ protocols, and business processes of the smart grid. This means they ~~are specific to none~~apply to most PAPS already formed or that will be formed hereafter.

11. **Has this cross PAP effect been discussed by the SGAC evaluation team?**

Yes, this cross-PAP effect has been discussed.

12. **What action items resulted from team discussions?**

Action Item	Assigned to	Status
~~TBD~~None		

(Add rows as needed)

13. **If there are use cases related to the standard, are the use cases and the standard aligned? Are these current/past use cases? Are they white box/black box? Are there future use cases or requirements?**

Much of this report is a catalogue of use cases, i.e., interactions and potential security risks. A potential concern with this report potential misuse. In a regulated market such as that for energy, a description can turn, by regulatory reference, into a requirement.

As the Architecture develops, recognition of some of the vulnerabilities identified herein may eliminate some or modify some interactions. Communication of that developing Architecture back to the Cybersecurity Team will then provide more concrete guidance for future implementations.

This report must communicate issues with legacy technology and installations even as it looks to the future. Some issues in legacy systems will not be solved while those systems and technologies persist.

In a future version of this report (work on which begins soon), it would be useful to identify interactions and associated risks based on the developing architecture, and encourage practitioners to move with all due speed to new applications that are secure by design..

14. **If there are use cases, are they candidates for the Conceptual Architecture – Requirements Document? If not present, what new requirements may need to be added?**

No new use cases for the conceptual architecture were discovered in this report.

15. **Is the terminology reasonably understandable by the intended audience? Is the terminology consistent through the document? Are standard dictionary(ies) referenced normatively?**

The report uses common language well understood in the industry. Most terms are defined within charts and columns that themselves serve as a dictionary to eliminate ambiguity.

16. **If UML class or other diagrams are useful for understanding the standard, are they available or used in the standard?**

Not applicable

17. **Does the standard include transitional artifacts? If so, are the transitional artifacts necessary to support legacy applications? Can they ever go away?**

The security architecture is not attempting to define future business practices, but to apply security to existing and probable future business practices. As such, it codifies issues that persist as long as current systems and business practices exist.

A future update to the report would be better if it identified business practices that, from a security perspective, would be candidates for transition.

18. **Are there things in the standard that have no obvious purpose in the use of the standard? Why do we think they're there? Are those things supporting evolution of application architectures?**

There are no aspects with no obvious purpose in the report.

19. **This standard is:**

A. A new standard that is being created by a new working group

B. A new standard that is being created by a new working group

C. A new standard that is being created by an established working group

D. A standard that was in draft form, but not finalized yet

E. A standard that was released but does not have a testing and conformance plan

F. A standard that is released, has a testing and conformance plan, but is undergoing a major revision

G. A standard that is mature, has testing and conformance and no major revisions are pending

The report is a catalogue of issues and potential security issues. It might be similar to [C], but the categories do not readily apply.

20. **Does this Standard limit options for innovation in the future? How? If yes, what limits are placed on innovation?**

Two significant purposes of the Architectures of the SG are to reduce attack surfaces and to reduce dependencies between applications and functions. By cataloging end-to-end issues linked to existing business models, the report potentially limits newer solutions which do not have the same end-to-end issues.

The report identifies some issues which are tied to particular market structures and current praxis. As long as the reader takes these as information about issues rather than requirements for future applications, then they will not inhibit innovation. The Cybersecurity committee has made note of those pointed out during this review, and plans to minimize these in future versions.

In particular, some current business practices prohibit sharing information in ways that would ease the entrance of new participants; these are catalogued in this report. Such sharing of information may be the essence of successful future smart energy deployments. There are use cases for live exchange of energy usage within the building, as well as a PAP (17) whose sole purpose is to codify such exchanges. Other applications, and other business models, or even other regulations may encourage or mandate sharing similar information. An exclusive focus on the security aspects of sharing under current business models might discourage the development of innovative technologies and business processes.

21. Other Comments:

Specific architectural concerns which should be addressed in the next version.

Comments on Volume 1L High Level Requirements

Comments on Figure 2-3, Logical Reference Model

- U56 appears to penetrate the ESI to perform cross-domain direct control. This is a logical interaction and not a direct one.

- 25L Distributed Generation and Storage Management should be either behind a premises ESI or use its own restricted ESI.

- U70 penetrates the ESI to perform direct plant control. This is a logical interaction and not a direct one.

- There appear to be many direct interactions on the left side of 41 (Aggregator / Retail Energy Provider). While these are intended to be logical, the graphic could be misinterpreted. Work in PAP09 states that all such interactions should be mediated through ESI and must support recursion.

- Need definition of ESI for U11 (DR management to Distribution Management)

- U106 appears to bypass the premises ESI to interact directly with Customer Energy Management System. While these are logical interactions, it should be noted that making them direct introduces additional security concerns and violates the consensus from PAP09 that all such interactions should be mediated through ESI.

~~Comments on Table 2-1, Actors~~

- ~~Actor 17 (GIS) is too specific (Utilities); there is extensive praxis for the security needs of Wide Area Situation Awareness (WASA), particularly in Emergency Management. It would be useful to reference that work to expand the perspective of readers.~~

- ~~Actor 44 (3rd Party) is too specific, and ignores recursion and other options and thus might limit examination of Security use cases.~~

Comment on Key Concepts and Assumptions

- Implied hierarchy in availability and resilience eliminates potential peer to peer negotiations between microgrids. Microgrid models (see Galvin "Perfect Power"-- http://www.galvinpower.org/) suggest that availability starts in a local microgrid and that resilience is gained by aggregating and interconnecting those microgrids. The reviewer has spent much of his career operating inside such a microgrid, and knows these interactions are not just theoretical. We suggest that a future version include a section that addresses security and resilience from the bottom-up microgrid perspective as well.

Comments on Table 2-2, Logical Interfaces

- Interface 10, interactions between control systems and non-control corporate systems uses as its sole example the interaction between two non-control systems (GIS and Work Management) in the same organization. Wide Area situation awareness is often shared between business entities; such information should be specified and secured in accord with principles of SOA Security. Examples of such interactions might include exchange of WASA between provider and aftermarket consumer (Coop or Aggregator), between Utility and Emergency Management, or between adjacent bulk providers.

  The SGAC would like to see a future version of this report extend the security analysis ~~of this area expanded~~ to include cases where the information exchanges cross organizational boundaries.

- Interface 17: see comments on Interface 10.

~~Comment on Figure 2-4, Logical Interface 1:~~

- ~~Consider issues if Actor 17 (GIS) is implemented as distributed GIS Services rather than as a monolithic GIS system.~~

Comments on section 2.3.5 – Logical Interface Category 9

- ~~The security model (as opposed to the security requirements) for today's insular market interactions are not necessarily a model for a market of a dynamic set players and recursive interactions that smart energy may require.~~

  Recommends that the assumptions in Bullet 9 be examined to include scenarios including dynamic discovery of markets, dynamic entry into markets, and dynamic exit from markets. While such activities are prohibited by today's market rules, they may be required to support microgrids, are anticipated by specifications already accepted into the catalog of standards.

~~Comments on section 2.3.6 –Logical Interface Category 10~~

- ~~Bullet 7 appears to assume interactions with GIS systems that are more monolithic than today's best practices. Consider in light of interoperation with distributed GIS services and interactions with less exceptional (purpose-built) systems.~~

  ~~A significant tactic to accelerate smart grid efforts is to adopt best practices from other areas where they exist. For GIS, these are not in IEC CIM or in NRECA, but in the domain experts, the Open Geospatial Consortium (OGC). The SGAC recommends that a future version of the report consider applying the models developed in OWS and related specifications to this space.~~

  ~~(This is related to the comments on WASA above).~~

- ~~Figure 2-13 appears to create possibility of cascading errors failures through successive re-integration of WASA from SCADA and Distribution Management. Recommend architecture that is less implementation specific and without cascading interactions. See GIS above.~~

Comments on section 2.3.8 –Logical Interface Category 12

- See comments on figure 2-13, GIS above.

Comments on section 2.3.~~1.2~~12 – Logical Interface Category 16

- Bullet 4: describes securing knowledge of interactions and information within a microgrid from that microgrid.

  > *Some information exchanged among different appliances and systems must be treated as confidential and private to ensure that an unauthorized third party does not gain access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential from other appliances whose vendors may want to scavenge this information for marketing purposes.*

  This is architecturally problematic because it violates the minimal interaction rule while blocking the ability of a microgrid to control and manipulate its own resources. ~~That occulting of interaction makes it more difficult to detect and ameliorate security breaches. The premise~~The premises / microgrid executes its internal commands and owns its internal data, and can share it as it wills. Propose that a future version modify this bullet similar to:

  > *Some information exchanged among different appliances and systems must be treated as confidential and private to ensure that an unauthorized third party does not gain*

access to it. For instance, energy usage statistics from the customer site that are sent through the ESI/HAN gateway must be kept confidential.

This removes what appears to be a blanket prohibition on internal [to the premises/microgrid] access to operational information

- Many bullets suggest multiple “through the interface” interactions. While this describes the interactions of today, the mode of design creates the possibility of multiple security issues.

  ~~From the SGAC perspective, this is bad architecture, which we believe results in bad security characteristics. We recommend that~~ We recommend that a future version of the report note this issue, and recommend that new implementations minimize such interactions.

~~- Bullet 11 – speaks to the architectural premise of minimal knowledge, and thereby to the security principle of minimal trust. This should be emphasized throughout this category.~~

~~General issue on Sections 2.3.1.2 and 2.3.1.3~~

~~- While it may be of use to particular market players to preserve exclusive access to their customers, it is a poor use of national policy to include this in requirements. “Prevent [competitor] access to information that could be used for marketing” and “present customer information for upsell” are business practices entirely orthogonal to smart grid activities, and should not be part of national smart grid requirements. They introduce unnecessary application and architecture constraints.~~

~~Section 3.1: High Level Security~~

~~- The SGIP Architecture makes no assumptions of a particular corporate structure or of particular corporate entities. Inclusion of “General Corporate Information” in smart grid security, particularly if the document is treated as having regulatory effect, can create conflicting directives and confusion, potentially reducing security. Suggest removing non-smart grid requirements.~~

22. SGAC Summary Comments:

~~*Smart Grid Architectural Overview*~~

At the highest level, the architecture of the smart grid is segmented into the domains Operations, Markets, Service Provider, Customer, Generation, Transmission, Distribution, and Customer. To the extent possible, these domains communicate with each other through minimal messages, and have minimal interactions across the inter-domain boundaries. This architecture is necessary to support the growing diversity of technology and process that is both a necessary enabler and a result of the rapid innovation needed to meet national goals.

~~At a more detailed level, the smart grid architecture is recursive; each grid can be composed from a number of microgrids, and each smart microgrid replicates the architecture of the overall smart grid. A customer interface may front a home or commercial building, or an office park or military base. The office park and military base may contain their distribution network, their own generation, and their own customer nodes. There is no architectural limit on this recursion; recent commercial products provide room-level micrograds that support a single service, and manage generation, storage, and distribution internally.~~

~~The Smart Grid Architecture addresses this diversity change by limiting direct interactions across each interface between domains. Management of generation, storage, and load is by service request; the resource providing the service may be a device, an aggregation of devices, or a virtual service. The energy services interface accepts requests for load response, for generation, for storage, and manages its internal operations.~~

~~*Security Implications of Architecture*~~

~~The architecture requires that there be no direct tunneling of directives through any interface. The architecture also implies that internal control of message handling is the responsibility of the microgrid, not of the larger grid that contains it. Specific micrograds may have different security requirements than the grids they participate in. Any interaction or requirement that directly crosses the energy services interface not only violates the architecture and introduces additional impedance of innovation, but it is a security violation the introduces potential vectors for security breaches. Each such architectural violation creates the possibility of "inadvertent compromises" as described in the report.~~

~~Each time an architectural boundary is penetrated, it reduces "defense in depth."~~

Architecturally, the answer to this challenge is to limit direct interactions across each interface between domains.

Interacting with Line of Business Applications

While core grid operations and interactions draw the most attention, the focus of the architecture on service interactions has implications for other areas of traditional "Utility Applications". These applications do and will exist for a long time.

The SGAC recommend that a future version of the report make recommendations about componentizing these applications in place to support better security over their life-times. For example, best practices in service oriented enterprises ~~is~~are to move toward common authentication and authorization mechanisms. These approaches are necessary at the intersection of Architecture and Security.

Interacting with GIS Systems

NISTIR 7628 sketches numerous interactions between GIS systems and line of business applications. Situation awareness on the grid involves collection and analysis of multiple rapidly changing datasets that are or can be tagged with geospatial positions.

The SGAC recommends that a future version of report reference existing work on Security in distributed GIS systems that can be found in the Open Geospatial Consortium (OGC), especially in interagency information sharing and in emergency management.

Users of the NISTIR working with geospatial systems may wish to review OGC work on sharing geospatial data and wide-area situation awareness. Just as in the NISTIR, the OGC does not endorse any particular approach, but tests test and document various best practices related to the OGC web services (and encodings) in various security environments.

2009 Geospatial eXtensible Access Control Markup Language (GeoXACML): http://www.opengeospatial.org/standards/geoxacml This is an OGC standard.

2011 OGC Authentication Interoperability Experiment
http://www.opengeospatial.org/projects/initiatives/authie (overview)
http://portal.opengeospatial.org/files?artifact_id=41734 (report)

2009 OWS-6 Secure Sensor Web Engineering Report
http://portal.opengeospatial.org/files/?artifact_id=34273 - This Engineering Report introduces standards-based security solutions for making the existing OGC Sensor Web Services, as described in the OWS-6 SWE baseline, ready towards the handling of sensors in the intelligence domain.

2009 OWS-6 Security Engineering Report:
http://portal.opengeospatial.org/files/?artifact_id=35461
This Engineering Report describes work accomplished during the OGC Web Services Test bed, Phase 6 (OWS 6) to investigate and implement security measures for OGC web services. This work was undertaken to address requirements stated in the OWS-6 RFQ/CFP originating from a number of sponsors, from OGC staff, and from OGC members.

2010 OWS-7 - Towards secure interconnection of OGC Web Services with SWIM:
http://portal.opengeospatial.org/files/?artifact_id=40144
This Engineering Report provides guidance and generate action items for the OGC standardization effort to properly enable security in the near future such that a seamless, interoperable but secure interconnection between OGC Web Services and FUSE ESB technology stack as selected by use in the System Wide Information

Management (SWIM) System of the US Federal Aviation Administration (FAA) can be achieved.

2007: Trusted Geo Services IPR: http://portal.opengeospatial.org/files/?artifact_id=20859
The OGC Trusted Geo Services Interoperability Program Report (IPR) provides guidance for the exchange of trusted messages between OGC Web Services and clients for these services. It describes a trust model based on the exchange and brokering of security tokens, as proposed by the OASIS WS-Trust specification [http://docs.oasis-open.org/ws-sx/ws-trust/200512].